Claims

What is claimed is:

1. A method for generating a random number, comprising the steps of:

marking an input signal to a flip-flop using a marking signal, wherein said input signal has a first binary value and a second binary value and wherein said marking signal marks approximately half of said first binary value as said first binary value and approximately half of the first binary value are marked as said second binary value;

decorrelating said marking signal to noise;

operating said flip-flop in a meta-stable state; and

generating a random bit from the marking signal based on the occurrence of the meta-stable state.

2. The method of claim 1, wherein said decorrelating step is performed by at least one linear feedback shift register.

3. The method of claim 2, wherein said linear feedback shift register provides a sufficient number of bits to decrease the chance of correlation.

4. The method of claim 2, wherein said linear feedback shift register (LFSR) provides a sufficient number of bits to reduce any bias in the LFSR output.

5. The method of claim 2, wherein said linear feedback shift register has a compensation circuit that removes bias from the generated random bits.

6. The method of claim 1, wherein said decorrelating step is performed by a collection of linear feedback shift registers.

7. The method of claim 1, wherein said flip-flop is placed in said meta-stable state by violating a set-up time of said flip-flop.

8. The method of claim 1, wherein said flip-flop is placed in said meta-stable state by violating a hold time of said flip-flop.

9. The method of claim 1, wherein said generating step further comprises the step of generating a mistake signal if an output of said flip-flop does not match an applied input.

10. The method of claim 9, wherein the mistake signal causes a random bit to be acquired based on the marking input.

11. The method of claim 1, further comprising the step of synchronizing an output of said flip-flop with a local clock source.

12. The method of claim 1, further comprising the step of collecting a plurality of said random bits to produce a random number.

13. The method of claim 1, wherein said first binary value is zero and said second binary value is one.

14. The method of claim 1, wherein said first binary value is one and said second binary value is zero.

15. The method of claim 1, further comprising the step of releasing collected bits from a shift register to generate said random bit.

16. A method for generating a random number, comprising the steps of:

marking an input signal to a flip-flop such that half of the zeroes are marked as zeroes and half of the zeroes are marked as ones and half of the ones are marked as zeroes and half of the ones are marked as ones;

decorrelating said marking signal to noise;

operating said flip-flop in a meta-stable state; and

generating a random bit from the marking signal based on the occurrence of said meta-stable state.

17. The method of claim 16, wherein said decorrelating step is performed by a linear feedback shift register.

18. The method of claim 17, wherein said linear feedback shift register provides a sufficient number of bits to decrease the chance of correlation.

19. The method of claim 17, wherein said linear feedback shift register (LFSR) provides a sufficient number of bits to reduce any bias in the LFSR output.

20. The method of claim 17, wherein said linear feedback shift register has a compensation circuit that removes bias from the generated random number.

21. The method of claim 16, wherein said decorrelating step is performed by a collection of linear feedback shift registers.

22. The method of claim 16, wherein said generating step further comprises the step of generating a mistake signal if an output of said flip-flop does not match an applied input.

23. The method of claim 16, further comprising the step of collecting a plurality of said random bits to produce a random number.

24. A random number generator, comprising:

a flip-flop operated in a meta-stable state;

a marking circuit for marking an input signal to said flip-flop using a marking signal, wherein said input signal has a first binary value and a second binary value and wherein said marking signal marks approximately half of said first binary value as said first binary value and approximately half of the first binary value are marked as said second binary value;

at least one linear feedback shift register that decorrelate said marking signal to noise; and

means for generating a random bit from the marking signal based on the occurrence of the meta-stable state.

25. The random number generator of claim 24, wherein said first binary value is zero and said second binary value is one.

26. The random number generator of claim 24, wherein said first binary value is one and said second binary value is zero.

27. The random number generator of claim 24, wherein said one or more linear feedback shift registers provide a sufficient number of bits to decrease the chance of correlation.

28. The random number generator of claim 24, wherein said one or more linear feedback shift registers (LFSRs) provide a sufficient number of bits to reduce any bias in the LFSR output.

29. The random number generator of claim 24, wherein said one or more linear feedback shift registers has a compensation circuit that removes bias from the generated random number.

30. A random number generator, comprising:

a flip-flop operated in a meta-stable state;

a marking circuit for marking an input signal to said flip-flop such that half of the zeroes are marked as zeroes and half of the zeroes are marked as ones and half of the ones are marked as zeroes and half of the ones are marked as ones;

one or more linear feedback shift registers that decorrelate said marking signal to noise; and

means for generating a random bit from the marking signal based on the occurrence of the meta-stable state.

31. The random number generator of claim 30, wherein said one or more linear feedback shift registers provide a sufficient number of bits to decrease the chance of correlation.

32. The random number generator of claim 30, wherein said one or more linear feedback shift registers (LFSRs) provide a sufficient number of bits to reduce any bias in the LFSR output.

33. The random number generator of claim 30, wherein said one or more linear feedback shift registers has a

compensation circuit that removes bias from the generated random number.